Scalar Polynomial Functions on the $n \times n$ Matrices over a Finite Field

J. V. Brawley*
Clemson University
Clemson, South Carolina

L. Carlitz†
Duke University
Durham, North Carolina

and

Jack Levine
North Carolina State University,
Raleigh, North Carolina

Recommended by A. S. Householder

ABSTRACT

Let $F = GF(q)$ denote the finite field of order q, and let $f(x) \in F[x]$. Then $f(x)$ defines, via substitution, a function from $F_{n\times n}$, the $n \times n$ matrices over F, to itself. Any function $f: F_{n\times n} \to F_{n\times n}$ which can be represented by a polynomial $f(x) \in F[x]$ is called a *scalar polynomial function* on $F_{n\times n}$. After first determining the number of scalar polynomial functions on $F_{n\times n}$, the authors find necessary and sufficient conditions on a polynomial $f(x) \in F[x]$ in order that it defines a permutation of (i) $\mathfrak{D}_n$, the diagonalizable matrices in $F_{n\times n}$, (ii) $\mathfrak{R}_n$, the matrices in $F_{n\times n}$ all of whose roots are in F, and (iii) the matric ring $F_{n\times n}$ itself. The results for (i) and (ii) are valid for an arbitrary field F.

1. PRELIMINARIES

Let $F = GF(q)$ denote the finite field of order q so that $q = p^r$ for some prime p and integer $r > 0$. It is well known [3] that any function $f: F \to F$ can be represented by a polynomial with coefficients in F. More precisely, f can

*Supported in part by ONR contract N00014-71-A-0339-0002.
†Supported in part by NSF grant GP-17031.

be represented by a unique polynomial of degree less than q. Conversely, if R is a commutative ring with identity such that every function $f: R \to R$ has a polynomial representation $f(x) = \sum a_i x^i$, $a_i \in R$, then R is necessarily a finite field [7, p. 507]. Recently it has been proved [1] that a ring R with identity (not necessarily commutative) has the property that every function from R to R can be represented by a *generalized* polynomial iff R is isomorphic to the ring $F_{n\times n}$ of $n \times n$ matrices over F for some n and some finite field F. By a generalized polynomial is meant a finite sum of terms of the type

$$A_0 x^{e_1} A_1 x^{e_2} \cdots A_{k-1} x^{e_k} A_k, \tag{1.1}$$

where $A_i \in R$, $e_i > 0$ and $k \geqslant 0$ but arbitrary. Thus every function from $F_{n\times n}$ to $F_{n\times n}$, $F = GF(q)$, has a representation as a generalized polynomial, but (unless $n = 1$) not as an ordinary polynomial $f(x) \in F[x]$.

If in (1.1) we replace each A_i by a scalar matrix $A_i = a_i I$, where $a_i \in F$ and I is the $n \times n$ identity matrix, we obtain an ordinary (scalar) polynomial which determines a function from $F_{n\times n}$ to $F_{n\times n}$.

DEFINITION. Let F be a field and let $n \geqslant 1$ be an integer. A function $f: F_{n\times n} \to F_{n\times n}$ is called a *scalar polynomial function* iff there exists a polynomial $f(x) \in F[x]$ which represents f via substitution of x by a matrix $A \in F_{n\times n}$. A polynomial $f(x) \in F[x]$ is called a *scalar polynomial.*

Thus every scalar polynomial is a generalized polynomial, but not conversely, and some but not all functions from $F_{n\times n}$ to $F_{n\times n}$ $(n > 1)$ are scalar polynomial functions.

DEFINITION. Let S be a subset of $F_{n\times n}$, F a field. A scalar polynomial $f(x) \in F[x]$ is called a *permutation polynomial* (abbreviated p.p.) on S iff it defines a one-one function of S onto itself.

In this paper we study scalar polynomial functions on $F_{n\times n}$. Throughout the paper, unless otherwise stated, F will denote the finite field $GF(q)$. In Sec. 2, we make some elementary observations concerning scalar polynomial functions on $F_{n\times n}$, and in Sec. 3, after first determining the monic $L_n(x) \in F[x]$ of least degree satisfied by every $A \in F_{n\times n}$, we enumerate the scalar polynomial functions on $F_{n\times n}$. Sections 4 and 5 contain theorems giving necessary and sufficient conditions on a scalar polynomial in order that it be a p.p. respectively on the diagonalizable matrices over F and the matrices over F whose roots lie in F. Here F is an arbitrary field. Using these results we construct in Sec. 5 a class of scalar polynomials which are p.p. on $F_{n\times n}$, $F = GF(q)$. In Secs. 6 and 7 we find necessary and sufficient conditions on a polynomial in order that it represent a p.p. on $F_{n\times n}$. The approach in Sec. 6 is matric theoretic, while in Sec. 7 we prove the same results using only facts concerning polynomials.

2. SOME ELEMENTARY OBSERVATIONS

Let $f(x)\in F[x]$, F an arbitrary field. If $A=aI$ is a scalar matrix, then clearly $f(aI)=f(a)I$. More generally if $D=\operatorname{diag}(d_1,\ldots,d_n)$ then $f(D)=\operatorname{diag}(f(d_1),\ldots,f(d_n))$. It is also clear that the image of a symmetric matrix under f is symmetric, and that the image of an upper (lower) triangular matrix is upper (lower) triangular. Since $P^{-1}f(A)P=f(P^{-1}AP)$ for all $A,P\in F_{n\times n}$, P nonsingular, it follows readily that if A is diagonalizable, then so is $f(A)$, and if A has all its roots in F, then so does $f(A)$, as A is similar to an upper triangular matrix. Moreover, if B commutes with A it commutes with $f(A)$. These facts will be used freely in the paper.

A few words concerning scalar permutation polynomials are in order. It is clear that the linear polynomial $ax+b\in F[x]$, $a\neq 0$, is a p.p. on $F_{n\times n}$ for all n. It is not clear whether or not there are scalar p.p. on $F_{n\times n}$ other than the linear ones. (We will see that there are indeed others for F finite.) However, the following result is fairly obvious.

THEOREM 1. *Let $f(x)\in F[x]$ be a permutation polynomial on $F_{n\times n}$. Then $f(x)$ is a permutation polynomial on $F_{m\times m}$ for all $m\leqslant n$. Moreover, if $n\geqslant 2$ then the coefficient of x in $f(x)$ is nonzero.*

Proof. To see that $f(x)$ is one-one on $F_{m\times m}$, assume $f(A)=f(B)$ for $A,B\in F_{m\times m}$, $m\leqslant n$. Then $f(\bar{A})=f(\bar{B})$ for $\bar{A}=\operatorname{diag}(A,0)$, and $\bar{B}=\operatorname{diag}(B,0)$, where 0 is $(n-m)\times(n-m)$. Thus $\bar{A}=\bar{B}$, so $A=B$. To show that $f(x)$ maps $F_{m\times m}$ onto $F_{m\times m}$, let $A\in F_{m\times m}$. There is a unique $X\in F_{n\times n}$ such $f(X)=\operatorname{diag}(A,0)$, where 0 is $(n-m)\times(n-m)$. For $Q=\operatorname{diag}(I,P)$, $P\in GL(n-m,F)$, it follows that $f(Q^{-1}XQ)=\operatorname{diag}(A,0)$; hence $Q^{-1}XQ=X$, implying $X=\operatorname{diag}(X_{11},X_{22})$, where $X_{11}\in F_{m\times m}$. Thus $f(X_{11})=A$. If $n\geqslant 2$ and $f(x)$ is a p.p. on $F_{n\times n}$, it is a p.p. on $F_{2\times 2}$. Now $g(x)=f(x)-f(0)$, $0\in F$, is a p.p. on $F_{n\times n}$ and $F_{2\times 2}$. Since for $A=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ and $B=\begin{pmatrix}0&1\\0&0\end{pmatrix}$, we have $g(A)=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ and $g(B)=\begin{pmatrix}0&a_1\\0&0\end{pmatrix}$, where a_1 is the coefficient of x in $f(x)$, it follows that $a_1\neq 0$. ∎

There are no polynomials in $F[x]$ other than the linear ones which are p.p. of $F_{n\times n}$ for all n. This result follows from

THEOREM 2. *Let F be a field, let $n\geqslant 1$ be an integer and let $f(x)\in F[x]$ be a permutation polynomial on $F_{n\times n}$. Then $f(x)$ has exactly one linear factor (in $F[x]$) and no other factor of degree less than $n+1$. If $n\geqslant 2$ the linear factor is of multiplicity 1.*

Proof. Since $f(x)$ is a p.p. on $F_{n\times n}$, it is a p.p. on $F = F_{1\times 1}$; thus $f(x)=0$ has exactly one root $r\in F$. Thus $f(x)=(x-r)^k h(x)$, where $h(r)\neq 0$. If $h(x)$ has a factor $g(x)$ of degree m, $1\leqslant m\leqslant n$, then $f(rI_m)=f(C)=0$, where C is the companion matrix of $g(x)$. This contradicts the fact that $f(x)$ is one-one on $F_{m\times m}$. Finally, if $n\geqslant 2$ and $k\geqslant 2$, then $f(rI_2)=f(B)$, where B is the companion matrix of $(x-r)^2$, contradicting the fact that $f(x)$ is one-one on $F_{2\times 2}$. ∎

COROLLARY 1. *Let F be a field. A polynomial $f(x)\in F[x]$ is a permutation polynomial on $F_{n\times n}$ for all n iff $f(x)=ax+b$ for some $a,b\in F$, $a\neq 0$.*

Proof. If $f(x)\in F[x]$ has degree $m>1$, then $f(x)$ is not a p.p. on $F_{m\times m}$ by Theorem 2. ∎

COROLLARY 2. *If $F=\mathbf{C}$ (complex field), then $f(x)$ is a permutation polynomial on $\mathbf{C}_{n\times n}$ iff $f(x)$ is linear.*

Proof. If $f(x)$ is a p.p. on $\mathbf{C}_{n\times n}$, it is a p.p. on $\mathbf{C}$, hence $f(x)=z$ has exactly one solution for each $z\in\mathbf{C}$. This implies $f(x)$ is linear. ∎

COROLLARY 3. *If $F=\mathbf{R}$ (real field), there are no permutation polynomials on $F_{n\times n}$ for $n\geqslant 2$ except the linear polynomials.*

Proof. A real polynomial of degree greater than one factors into linear and irreducible quadratic factors over $\mathbf{R}[x]$. If $f(x)$ is a p.p. on $\mathbf{R}_{n\times n}$ $(n\geqslant 2)$, then by Theorem 2, $f(x)$ has exactly one linear factor and no quadratic factors. ∎

3. SCALAR POLYNOMIAL FUNCTIONS ON $F_{n\times n}$

In this section we prove that every scalar polynomial function from $F_{n\times n}$ to $F_{n\times n}$ $(F=GF(q))$ is representable by a unique polynomial $f(x)\in F[x]$ of degree less than

$$\delta = q^n + q^{n-1} + \cdots + q = q(q^n-1)/(q-1). \tag{3.1}$$

This result follows easily from the next theorem.

THEOREM 3. *Let $F=GF(q)$, let $n>0$ be an integer, and let*

$$L_n(x) = \prod_{k=1}^{n} (x^{q^k}-x). \tag{3.2}$$

Then $L_n(A)=0$ for all $A\in F_{n\times n}$; indeed, $L_n(x)$ is the monic of least degree which enjoys this property.

Proof. For $A\in F_{n\times n}$ put $C_A(x)=\det(xI-A)$, and define $L(x)$ by

$$L(x)=\operatorname*{L.C.M.}_{A\in F_{n\times n}}\{C_A(x)\}.$$

Then $L(A)=0$ for all $A\in F_{n\times n}$ as $C_A(A)=0$. Thus denote by $L_n(x)$ the monic of least degree satisfied by every $A\in F_{n\times n}$, so that $L_n(x)|L(x)$. Since $\deg C_A(x)=n$ and since every polynomial $Q(x)\in F[x]$ of degree n is the characteristic polynomial for some $A\in F_{n\times n}$, we have

$$L(x)=\operatorname*{L.C.M.}_{\deg Q=n}\{Q(x)\}.$$

But every $Q(x)$ of degree n is the minimum polynomial of its companion matrix, so that $Q(x)|L_n(x)$ for all $Q(x)\in F[x]$; hence $L_n(x)=L(x)$.

If $P(x)$ is an irreducible factor of $Q(x)$, where $\deg Q(x)=n$, $\deg P(x)=k$, $P(x),Q(x)\in F[x]$, then $P(x)$ is a factor of $Q(x)$ of multiplicity at most $[n/k]$. Moreover, the degree n polynomial $x^{n-k[n/k]}P(x)^{[n/k]}$, where $P(x)$ is an arbitrary irreducible of degree $k\leqslant n$, has $P(x)^{[n/k]}$ as a factor; thus,

$$L_n(x)=\operatorname*{L.C.M.}_{\deg Q=n}\{Q(x)\}=\prod_{\deg P=k\leqslant n}P(x)^{[n/k]}, \tag{3.3}$$

where $P(x)$ is irreducible and monic.

To complete the argument, let $\theta\in GF(q^k)$ be a root of $P(x)=0$, where $P(x)$ is an irreducible of degree $k\leqslant n$ in $F[x]$. Then θ is a root of $L_n(x)$ exactly $[n/k]$ times. But θ is also a root of $\prod_{t=1}^{n}(x^{q^t}-x)$ exactly $[n/k]$ times, as θ satisfies exactly one each of $x^{q^k}-x$, $x^{q^{2k}}-x,\ldots,x^{q^{[n/k]k}}-x$, and these are the only factors satisfied by θ. Hence

$$L_n(x)=\prod_{k=1}^{n}(x^{q^k}-x),$$

as both sides have exactly the same roots with the same multiplicites. A proof of the fact that L.C.M. $\{Q(x)\}=\prod(x^{q^k}-x)$ also appears in [2]. ∎

THEOREM 4. *Let $F=GF(q)$. Each scalar polynomial function from $F_{n\times n}$ to $F_{n\times n}$ is representable by a unique polynomial $f(x)\in F[x]$ of degree less than $\delta=q^n+\cdots+q^2+q$. The number of scalar polynomial functions on $F_{n\times n}$ is q^δ.*

Proof. Let $g(x) \in F[x]$. Then $g(x) = f(x) + L_n(x)h(x)$, where $\deg f(x) < \deg L_n(x) = \delta$. By Theorem 3, $g(A) = f(A)$ for all $A \in F_{n\times n}$, so that the scalar polynomial function defined by $g(x)$ is representable by a polynomial $f(x)$ of degree less than δ. If $f(x)$ and $f_0(x)$ are of degree less than δ and represent the same scalar polynomial function, then $d(x) = f(x) - f_0(x)$ satisfies $d(A) = 0$ for all A, so that $L_n(x) | d(x)$, implying $d(x) = 0$ or $f(x) = f_0(x)$. The number of polynomials in $F[x]$ of degree less than δ is clearly q^δ. ∎

An interesting question which the authors have not considered is the following: What are necessary and sufficient conditions on a function $f: F_{n\times n} \to F_{n\times n}$ in order that it have a scalar polynomial representation? Certainly a number of necessary conditions are easily obtained, as indicated by the first paragraph of Sec. 2.

We conclude this section with several remarks. Let S_n denote the semigroup of all scalar polynomial functions from $F_{n\times n}$ to $F_{n\times n}$ under composition. Theorem 4 gives $|S_n|$. Put

$$\mathfrak{S}_n = \{ f(x) \in F[x] : \deg f(x) < \delta \},$$

and define the operation $\circ$ on $\mathfrak{S}_n$ by

$$f(x) \circ g(x) = h(x),$$

where $h(x) \equiv f(g(x)) \pmod{L_n(x)}$. It is then clear that S_n and $\mathfrak{S}_n$ are isomorphic by the mapping $\Phi: \mathfrak{S}_n \to S_n$, where Φ is the evaluation mapping. A function $f(x) \in \mathfrak{S}_n$ is in the group of units $\mathfrak{G}_n$ of $\mathfrak{S}_n$—i.e., is a permutation polynomial—if and only if there is a function $g(x) \in F[x]$ such that

$$g(f(x)) \equiv x \pmod{L_n(x)} \tag{3.4}$$

or equivalently

$$f(g(x)) \equiv x \pmod{L_n(x)}. \tag{3.5}$$

These facts will be used in Sec. 7.

4. SCALAR POLYNOMIALS WHICH PERMUTE THE DIAGONALIZABLE MATRICES

One of the purposes of this paper is to give necessary and sufficient conditions on a polynomial $f(x) \in F[x]$ in order that it is a p.p. on $F_{n\times n}$, $F = GF(q)$. Of course such a polynomial necessarily permutes the diagonalizable matrices in $F_{n\times n}$. Thus as a first step toward accomplishing this purpose, we find conditions on $f(x)$ in order that it define a permutation of

$\mathfrak{D}_n = \mathfrak{D}_n(F)$, the diagonalizable matrices over F. Here F is an arbitrary field, and as might be expected we have the following result.

THEOREM 5. *Let $f(x) \in F[x]$, F a field, The following are equivalent:*

1. *$f(x)$ is a permutation polynomial on $\mathfrak{D}_n(F)$ for all n.*
2. *$f(x)$ is a permutation polynomial on $\mathfrak{D}_n(F)$ for some $n \geqslant 1$.*
3. *$f(x)$ is a permutation polynomial on F.*

Proof. Clearly 1 implies 2. Also, if $f(x)$ is a p.p. on $\mathfrak{D}_n(F)$ for some $n \geqslant 1$, then f is a one-one function on $\mathfrak{D}_1(F)$; for if $f(a) = f(b)$, then $f(aI) = f(bI)$ where I is $n \times n$, implying $aI = bI$ or $a = b$. Moreover, if $a \in F$, there is an $X \in \mathfrak{D}_n(F)$ such that $f(X) = aI$. Hence for all $P \in GL(n, F)$, $P^{-1}f(X)P = f(P^{-1}XP) = P^{-1}(aI)P = aI$ or $P^{-1}XP = X$, showing that X is a scalar matrix $X = cI$. Thus $f(c) = a$, so that $f(x)$ is a p.p. on $\mathfrak{D}_1(F)$.

Thus, let $f(x)$ be a p.p. on F and let $n \geqslant 1$ be arbitrary. If $A \in \mathfrak{D}_n$, there is a P such that $P^{-1}AP = D = \operatorname{diag}(d_1, \ldots, d_n)$, and since $f(x)$ is a p.p. on F, there are elements $c_1, c_2, \ldots, c_n$ in F such that $f(c_i) = d_i$. Thus putting $C = \operatorname{diag}(c_1, c_2, \ldots, c_n)$, it follows that $f(C) = D$; hence $f(PCP^{-1}) = Pf(C)P^{-1} = A$. Thus f maps $\mathfrak{D}_n$ onto $\mathfrak{D}_n$. (In case F is finite, the proof is now complete, as onto implies one-one.) It remains to prove $f(x)$ is one-one; suppose for $A, B \in \mathfrak{D}_n$, $f(A) = f(B)$. There exists a matrix $P \in GL(n, F)$ such that

$$P^{-1}BP = \operatorname{diag}(b_1 I_{k_1}, \ldots, b_t I_{k_t}),$$

where $\sum k_i = n$ and $b_i \neq b_j$ for $i \neq j$. Also there is a $Q \in GL(n, F)$ such that

$$Q^{-1}(P^{-1}AP)Q = \operatorname{diag}(a_1 I_{r_1}, \ldots, a_m I_{r_m}), \tag{4.2}$$

where $\sum r_i = n$ and $a_i \neq a_j$ for $i \neq j$. Now $f(A) = f(B)$ implies $f(Q^{-1}P^{-1}APQ) = Q^{-1}f(P^{-1}BP)Q$ or

$$\operatorname{diag}(f(a_1)I_{r_1}, \ldots, f(a_m)I_{r_m}) = Q^{-1}\operatorname{diag}(f(b_1)I_{k_1}, \ldots, f(b_t)I_{k_t})Q. \tag{4.3}$$

Since similar matrices have the same characteristic roots, $m = t$ and there is some ordering of the b_i's such that $a_i = b_{s_i}$ and $r_i = k_{s_i}$, $i = 1, 2, \ldots, t$. (Note we have used the fact that $f(x)$ is one-one on F.) Without loss of generality, we may assume the matrix Q of (4.1) has been selected so that $a_i = b_i$ and $r_i = k_i$, $i = 1, 2, \ldots, t$; therefore (4.2) and (4.3) become respectively

$$Q^{-1}P^{-1}APQ = \operatorname{diag}(b_1 I_{k_1}, \ldots, b_t I_{k_t}) = D \tag{4.2'}$$

and

$$f(D) = Q^{-1} f(D) Q, \tag{4.3'}$$

where D is the diagonal matrix defined by (4.2'). From (4.3') it follows that Q commutes with $f(D) = \operatorname{diag}(f(b_1)I_{k_1}, \ldots, f(b_t)I_{k_t})$, from which it is easily deduced that Q has the partitioned form

$$Q = \operatorname{diag}(Q_1, Q_2, \ldots, Q_t),$$

where Q_i is $k_i \times k_i$. Hence, Q commutes with D, and from (4.2') we have $P^{-1}AP = QDQ^{-1} = D = P^{-1}BP$ or $A = B$. This completes the proof. ∎

COROLLARY 1. *The number of scalar polynomial functions from* $\mathfrak{D}_n(F)$ *to* $\mathfrak{D}_n(F)$, *where* $F = GF(q)$, *is* q^q, *and of these* $q!$ *are permutations of* $\mathfrak{D}_n(F)$.

Proof. Every $A \in \mathfrak{D}_n(F)$ satisfies $x^q - x = 0$, and $x^q - x$ is the monic of least degree satisfied by every $A \in \mathfrak{D}_n(F)$. Thus if $g(x) \in F[x]$ and $g(x) = f(x) + (x^q - x)h(x)$, where $\deg f(x) < q$, then $g(x)$ and $f(x)$ restricted to $\mathfrak{D}_n(F)$ represent the same function. Moreover, $g(x)$ is a permutation polynomial on F iff $f(x)$ is a permutation polynomial on F, and if $f(x)$ and $f_0(x)$ represent different functions on F, they represent different functions on $\mathfrak{D}_n(F)$. ∎

Of course, the point of view of Corollary 1 is to look at a given polynomial only as it acts on $\mathfrak{D}_n(F)$. Two polynomials $g(x)$ and $h(x)$ may act differently on $F_{n\times n}$ but the same on $\mathfrak{D}_n(F)$. To obtain the number of scalar polynomial functions on $F_{n\times n}$ which permute the elements of $\mathfrak{D}_n(F)$, consider

$$f_0(x) + (x^q - x)f_1(x),$$

where $\deg f_1(x) < q^n + q^{n-1} + \cdots + q^2$. For fixed $f_0(x)$ as $f_1(x)$ varies we obtain all different functions on $F_{n\times n}$ which behave like $f_0(x)$ on $\mathfrak{D}_n(F)$. Thus we have proved

COROLLARY 2. *The number of different scalar polynomial functions on* $F_{n\times n}$ *which permute* $\mathfrak{D}_n(F)$ *is* $q!q^\rho$, *where* $\rho = q^n + q^{n-1} + \cdots + q^2 = \delta - q$.

5. SCALAR POLYNOMIALS WHICH PERMUTE THE ROOT MATRICES

Let F be an arbitrary field and let $A \in F_{n\times n}$. The matrix A is called a *root matrix over* F iff all n of its characteristic roots lie in F. The set of all root matrices over F is denoted by $\mathfrak{R}_n = \mathfrak{R}_n(F)$. In the present section we find necessary and sufficient conditions on a polynomial $f(x) \in F[x]$ in order that it permute $\mathfrak{R}_n$. It is evident that $\mathfrak{D}_n \subseteq \mathfrak{R}_n$; thus, it is readily argued that if a polynomial $f(x) \in F[x]$ is a p.p. on $\mathfrak{R}_n$, it is a p.p. on $\mathfrak{D}_n$, and hence $f(x)$ is a p.p. on F. This condition is not sufficient, as we shall soon see. We begin with several lemmas.

LEMMA 1. *Let $a_0, a_1, a_2, \ldots$ be elements of F with $a_1 \neq 0$, and for each integer $n \geqslant 1$, let*

$$A_n = a_0 I_n + a_1 N_n + a_2 N_n^2 + \cdots + a_{n-1} N_n^{n-1}, \tag{5.1}$$

where N_n is the $n \times n$ Jordan matrix with 1's on the superdiagonal and 0's elsewhere. Then a $t \times k$ matrix X over F satisfies $A_t X = X A_k$ iff X satisfies $N_t X = X N_k$.

Proof. The general form of a matrix satisfying $N_t X = X N_k$ is well known [8, p. 144]. (Clearly any such matrix satisfies $A_t X = X A_k$.) It is a straightforward exercise using the same techniques as in [8] to show that the general form of a matrix satisfying $A_t X = X A_k$ is precisely the general form of a solution of $N_t X = X N_k$. ■

LEMMA 2. *Let $A = \operatorname{diag}(A_{k_1}, A_{k_2}, \ldots, A_{k_t})$ and $B = \operatorname{diag}(B_{k_1}, B_{k_2}, \ldots, B_{k_t})$, where the A_{k_i} have the form (5.1) based on a sequence $a_0, a_1, \ldots$ with $a_1 \neq 0$, and the B_{k_i} have the same form as (5.1) but based on a (possibly different) sequence $a_0, b_1, b_2, \ldots$, where $b_1 \neq 0$. Then X commutes with A iff it commutes with B.*

Proof. The proof is obvious, using partitioned matrices and Lemma 1. ■

LEMMA 3. *Let A_n be given by (5.1) (with $a_1 \neq 0$). Then A_n is similar to the Jordan matrix*

$$J_n(a_0) = a_0 I_n + N_n. \tag{5.2}$$

Proof. It is easily argued that the Smith normal form [see 6] for both matrices is diag $(1, 1, \ldots, 1, (x-a_0)^n)$. ∎

We are now ready to prove the main result of this section.

THEOREM 6. *Let $f(x) \in F[x]$, F a field. The following are equivalent:*

1. *$f(x)$ is a permutation polynomial on $\mathfrak{R}_n$ for all $n \geqslant 1$.*
2. *$f(x)$ is a permutation polynomial on $\mathfrak{R}_n$ for some $n \geqslant 2$.*
3. (i) *$f(x)$ is a permutation polynomial on F, and* (ii) *$f'(x)$ has no roots in F.*

Proof. If $f(x)$ is a p.p. on $\mathfrak{R}_n$ for all $n \geqslant 1$, it is a p.p. on $\mathfrak{R}_n$ for some $n \geqslant 2$. Thus assume $f(x)$ is a p.p. on $\mathfrak{R}_n$ for some $n \geqslant 2$, and let $m \leqslant n$. Clearly, $f(\mathfrak{R}_m) \subseteq \mathfrak{R}_m$; indeed this is true for any polynomial $f(x) \in F[x]$. In addition, if $A, B \in \mathfrak{R}_{m \times m}$ satisfy $f(A) = f(B)$, then $f(\mathrm{diag}(A, I_{n-m})) = f(\mathrm{diag}(B, I_{n-m}))$, so that $A = B$; hence $f(x)$ restricted to $\mathfrak{R}_m$ is one-one. To see that it is also onto, let $A \in \mathfrak{R}_m$ be arbitrary. Then there is a unique $X \in \mathfrak{R}_n$ such that $f(X) = \mathrm{diag}(A, I_{n-m})$. Thus for $Q = \mathrm{diag}(I, P)$, where $P \in GL(n-m, F)$, we have $f(Q^{-1}XQ) = \mathrm{diag}(A, I_{n-m})$, implying that $Q^{-1}XQ = X$ (for all P) and hence that $X = \mathrm{diag}(X_{11}, X_{22})$, where $X_{11} \in \mathfrak{R}_m$. Thus $f(X_{11}) = A$, so that $f(x)$ is a p.p. on $\mathfrak{R}_m$, and in particular on $\mathfrak{R}_1 = F$; hence (i) is valid. Moreover, since $f(x)$ is a p.p. on $\mathfrak{R}_2$, $f'(x)$ can have no roots in F; otherwise, if $f'(a) = 0$ for $a \in F$, then

$$f\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \begin{pmatrix} f(a) & f'(a) \\ 0 & f(a) \end{pmatrix} = \begin{pmatrix} f(a) & 0 \\ 0 & f(a) \end{pmatrix} = f\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

which is a contradiction. Hence (ii) is also valid. Thus assume that both (i) and (ii) hold, and let $n \geqslant 1$ be arbitrary. The proof will be complete if we show $f(x)$ is a p.p. on $\mathfrak{R}_n$.

To see that $f(x)$ is onto, consider first an arbitrary Jordan matrix $J_m(a)$ of the form (5.2). By (i) there exists $b \in F$ such that $f(b) = a$, and by (ii), $f'(b) \neq 0$. An easy computation shows that

$$f(J_m(b)) = b_0 I + b_1 N_m + \cdots + b_{m-1} N_m^{m-1},$$

where $J_m(b) = bI + N_m$ as in (5.2), $b_0 = f(b) = a$ and $b_1 = f'(b) \neq 0$. By Lemma 3, there is a $P \in GL(m, F)$ such that

$$P^{-1} f(J_m(b)) P = b_0 I + N_m = J_m(a);$$

hence $f(B) = J_m(a)$, where $B = P^{-1} J_m(b) P$. Now let $A \in \mathfrak{R}_n$ be arbitrary, and

let $Q \in GL(n,F)$ be a matrix which sends A to its Jordan canonical form; i.e.,

$$Q^{-1}AQ = \bar{A} = \operatorname{diag}\big(J_{k_1}(a_1),\ldots,J_{k_t}(a_t)\big).$$

Let $B_1, B_2,\ldots,B_t$ be matrices such that $f(B_i) = J_{k_i}(a_i)$, and set

$$B = Q\operatorname{diag}(B_1, B_2,\ldots,B_t)Q^{-1}.$$

Then $f(B) = Q\operatorname{diag}(f(B_1),\ldots,f(B_t))Q^{-1} = Q\bar{A}Q^{-1} = A$, so that $f(x)$ is onto. Again, if F is finite the proof is complete.

Finally, we must argue that $f(x)$ is one-one. Let $A, B \in \mathfrak{R}_n$ be such that $f(A) = f(B)$. There exist matrices P, $Q \in GL(n,F)$ such that

$$P^{-1}BP = \operatorname{diag}(B_1, B_2,\ldots,B_r) = \bar{B}, \tag{5.3}$$

$$Q^{-1}P^{-1}APQ = \operatorname{diag}(A_1, A_2,\ldots,A_s) = \bar{A}, \tag{5.4}$$

where

$$B_i = \operatorname{diag}\big(J_1^{(i)}(b_i), J_2^{(i)}(b_i),\ldots,J_{t_i}^{(i)}(b_i)\big)$$

is a sum of Jordan matrices (5.2) corresponding to the root b_i $(i = 1,2,\ldots,r)$, with $b_i \neq b_j$ if $i \neq j$. A similar statement holds for A, where the distinct roots of A are denoted by a_1, $a_2,\ldots,a_s$. Since $f(A) = f(B)$, $f(Q^{-1}P^{-1}APQ) = Q^{-1}f(P^{-1}BP)Q$ or

$$f(\bar{A}) = Q^{-1}f(\bar{B})Q, \tag{5.5}$$

so that $f(\bar{A})$ and $f(\bar{B})$ are similar. But

$$f(\bar{B}) = \operatorname{diag}(f(B_1),\ldots,f(B_r))$$

with

$$f(B_i) = \operatorname{diag}\Big(f\big(J_1^{(i)}(b_i)\big),\ldots,f\big(J_{t_i}^{(i)}(b_i)\big)\Big),$$

and where

$$f\big(J_k^{(i)}(b_i)\big) = f(b_i)I + f'(b_i)N + \ldots, \qquad k = 1, 2,\ldots,t_i$$

has the form (5.1) with $f'(b_i) \neq 0$. A like statement holds for $f(\bar{A})$. This means, by Lemma 3 and the fact that $f(x)$ is one-one on F, that $r = s$ and there is an ordering of the B_i's such that $A_i = B_{j_i}$. We assume the matrix Q of (5.4) is

selected so that $A_i = B_i$, $i = 1, 2, \ldots, r$. Hence $\bar{A} = \bar{B}$. From (5.5) with $\bar{B} = \bar{A}$, we have $Qf(\bar{A}) = f(\bar{A})Q$. Here $f(\bar{A}) = \operatorname{diag}(f(A_1), \ldots, f(A_r))$, where $f(A_i)$ is upper triangular with diagonal elements $f(a_i)$; thus, since $f(a_i) \neq f(a_j)$ for $i \neq j$, it follows that $Q = \operatorname{diag}(Q_1, \ldots, Q_r)$. Hence $Q_i f(A_i) = f(A_i)Q$ for each i. Since $f(A_i)$ and A_i $(i = 1, 2, \ldots, r)$ are of the form needed to apply Lemma 2, $Q_i f(A_i) = f(A_i)Q_i$ implies $Q_i A_i = A_i Q_i$; hence $Q = \operatorname{diag}(Q_1, \ldots, Q_r)$ commutes with $\bar{A} = \operatorname{diag}(A_1, \ldots, A_r)$. Therefore from (5.3) and (5.4) we have $P^{-1}AP = Q\bar{A}Q^{-1} = \bar{A} = \bar{B} = P^{-1}BP$ or $A = B$, and the proof is complete. ∎

Using Theorem 6 it is easy to obtain an alternate proof of Corollary 2 to Theorem 2. A much more interesting result is the next theorem.

THEOREM 7. *Let $F = GF(q)$, and let $E = GF(q^m)$, where $m = \text{L.C.M.}\{1, 2, \ldots, n\}$. Let $f(x)$ be a polynomial with coefficients in F $(f(x) \in F[x])$ such that*

(i) *$f(x)$ is a permutation polynomial on E, and*
(ii) *$f'(x)$ has no roots in E.*

Then $f(x)$ is a permutation polynomial on $F_{n\times n}$.

Proof. Note that E is the splitting field of $L_n(x)$ as given by (3.2). Thus any matrix $A \in F_{n\times n}$ has all of its roots in E; that is, $F_{n\times n} \subseteq \mathfrak{R}_n(E)$. By Theorem 6, $f(x)$ is a p.p. on $\mathfrak{R}_n(E)$, and since $f(F_{n\times n}) \subseteq F_{n\times n}$, it follows that $f(x)$ is a p.p. on $F_{n\times n}$. ∎

Theorem 7 allows us to exhibit some scalar permutation polynomials on $F_{n\times n}$ other than the linear polynomials. Of course, $ax + b$, $a \neq 0$ satisfies condition (i) and (ii) of Theorem 7.

EXAMPLE 1. Let $F = GF(2)$ and $n = 2$. Then $L_n(x) = (x^4 - x)(x^2 - x)$, so that all scalar polynomial functions may be assumed to have degree less than 6. Consider the polynomial $f(x) = x^4 + x^2 + x$. It is clearly a p.p. on $GF(2)$ and is easily seen to be a p.p. on $GF(2^2)$. Since $f'(x) = 1$, $f(x)$ satisfies the conditions in Theorem 7 and hence is a p.p. on $F_{2\times 2}$. Similarly, $f(x) + 1 = x^4 + x^4 + x + 1$ is a p.p. on $F_{n\times n}$. (Note that if $f(x)$ is a p.p. on $F_{n\times n}$, so is $f(x) + a$.) It has been verified by the authors that only four of the 16! permutations of $F_{2\times 2}$ are representable by polynomials, and these are the functions defined by x, $x + 1$, $x^4 + x^2 + x$, $x^4 + x^2 + x + 1$.

EXAMPLE 2. Let $F = GF(q)$ and let $n \geq 1$ be arbitrary. Consider the set $\mathfrak{S}$ of all polynomials $f(x)$ of the form

$$f(x) = a_0 x + a_1 x^q + a_2 x^{q^2} + \cdots + a_{m-1} x^{q^{m-1}}, \qquad a_i \in F, \tag{5.6}$$

where $m = \text{L.C.M. } \{1,2,\ldots,n\}$, $a_0 \neq 0$ and the circulant determinant

$$|C| = \begin{vmatrix} a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \\ a_{m-2} & a_{m-3} & \cdots & a_0 & a_{m-1} \\ \vdots & \vdots & & \vdots & \vdots \\ a_0 & a_{m-1} & \cdots & a_2 & a_1 \end{vmatrix}$$

is nonzero. Then $f(x)$ is a p.p. on E (see [3, p. 66]), and $f'(x) = 0$ has no roots in E, so that $f(x)$ is a p.p. on $F_{n\times n}$. The set $\mathcal{G}$ is a group under composition and is a subgroup of the Betti-Mathieu group [3, p. 64]. (It should be mentioned that polynomials of the form (5.6) with $p = q$ were studied by Ore in [4] and [5].) Of course if $f(x) \in \mathcal{G}$, then $f(x) + a$, $a \in F$, is also a p.p. on $F_{n\times n}$. Note that (5.6) can possibly be reduced modulo $L_n(x)$.

As a special case of Example 2, let $n = 2$, so that $m = 2$. Then for a_0, $a_1 \in GF(q)$ with $a_0 \neq 0$, $a_1 \neq \pm a_0$, the polynomial $a_0x + a_1x^q$ is a p.p. on $F_{2\times 2}$, $F = GF(q)$.

Although Theorem 7 gives sufficient conditions in order that $f(x)$ is a p.p. on $F_{n\times n}$, condition (ii) is too strong, as we will show in the next section.

6. SCALAR PERMUTATION POLYNOMIALS ON $F_{n\times n}$: A MATRIX APPROACH

We first derive two necessary conditions on a polynomial $f(x) \in F[x]$ in order that it be a permutation polynomial on $F_{n\times n}$, after which we show that these two conditions are indeed sufficient. Here $F = GF(q)$.

LEMMA 1. *Let $f(x) \in F[x]$ be a permutation polynomial on $F_{n\times n}$, and let $K = GF(q^t)$, where $1 \leqslant t \leqslant n$, so that $F \subseteq K$. Then $f(x)$ is a permutation polynomial on K.*

Proof. Clearly $f(K) \subseteq K$; hence it is sufficient to show that f is one-one. Since K is a finite extension of F, there exists $\theta \in K$ whose minimum polynomial $m(x)$ over F has degree t. Moreover, each $\alpha \in K$ is uniquely expressible in the form $\alpha = \sum_{i=0}^{t-1} a_i\theta^i$, where $a_i \in F$. Since $f(x)$ is a p.p. on $F_{n\times n}$, by Theorem 1, it is a p.p. on $F_{t\times t}$ as $t \leqslant n$; in particular, if $\mathcal{A}$ is the subalgebra of $F_{t\times t}$ generated by the companion matrix C of $m(x)$, then f is a p.p. on $\mathcal{A}$ as $f(\mathcal{A}) \subseteq \mathcal{A}$. Suppose then that $f(\alpha) = f(\beta)$, $\alpha, \beta \in K$. Since $\alpha = \sum a_i\theta^i$, $f(\alpha)$ may be computed from $f(\sum a_i\theta^i)$ by doing operations modulo

$m(\theta)$ to get

$$f(\alpha)=\sum_{i=0}^{t-1} c_i\theta^i.$$

Likewise, $\beta=\sum b_i\theta^i$ and $f(\beta)=\sum c_i\theta^i=f(\alpha)$. Define matrices $A,B\in\mathfrak{C}$ by $A=\sum a_iC^i$ and $B=\sum b_iC^i$. Then $f(A)=f(B)=\sum c_iC^i$, as the computations involved are modulo $m(C)$. Since $f(x)$ is a p.p. on $\mathfrak{C}$, $A=B$, and this implies $a_i=b_i$, $i=0,1,\ldots,t-1$; hence, $\alpha=\beta$. ■

LEMMA 2. *Let $f(x)\in F[x]$ be a permutation polynomial on $F_{n\times n}$, and let $K=GF(q^t)$ with $1\leqslant t\leqslant [n/2]$, where $[n/2]$ is the greatest integer in $n/2$. Then $f'(x)=0$ has no roots in K.*

Proof. Suppose to the contrary that $f'(x)=0$ has a root $\lambda\in GF(q^t)=K$, where $2t\leqslant n$. Let $m(x)$ be the minimum polynomial of λ over F, let $d=\deg m(x)$, and let C be the companion matrix of $m(x)$. Then $d|t$, as $F(\lambda)=GF(q^d)\subseteq GF(q^t)$. Put

$$A=\begin{pmatrix} C & 0\\ 0 & C\end{pmatrix},\qquad B=\begin{pmatrix} C & N\\ 0 & C\end{pmatrix},$$

where $N=(n_{ij})$ is $d\times d$ with $n_{d1}=1$ and $n_{ij}=0$ otherwise. Then A, $B\in F_{2d\times 2d}$. Since $2d\leqslant 2t\leqslant n$, $f(x)$ is a p.p. on $F_{2d\times 2d}$. Moreover, all the roots of A and B lie in K. Thus, there exist P, $Q\in GL(2d,K)$ which bring A and B to their respective Jordan forms; namely

$$P^{-1}AP=\operatorname{diag}(\lambda_1I_2,\lambda_2I_2,\ldots,\lambda_dI_2),$$

$$Q^{-1}BQ=\operatorname{diag}(J(\lambda_1),J(\lambda_2),\ldots,J(\lambda_d)),$$

where $\lambda=\lambda_1,\lambda_2,\ldots,\lambda_d$ are the roots of $m(x)=0$ in $GF(q^t)$ (conjugates of λ), I_2 is the 2×2 identity matrix, and $J(\lambda_i)=\lambda_iI_2+N_2$. Since $f'(\lambda_i)=0$, $i=1,2,\ldots,d$, it follows that $f(P^{-1}AP)=f(Q^{-1}BQ)$ or $(QP^{-1})f(A)(pQ^{-1})=f(B)$, showing that $f(A)$ and $f(B)$ are similar over K. But then $f(A)$ and $f(B)$ are similar over F[6, p. 144], so there exists $R\in GF(2d,F)$ such that $R^{-1}f(A)R=f(B)=f(R^{-1}AR)$. Hence $R^{-1}AP=B$ as $f(x)$ is a p.p. on $F_{2d\times 2d}$. This is a contradiction as A,B are not similar. ■

THEOREM 8. *Let $f(x)\in F[x]$, $F=GF(q)$. Then $f(x)$ is a permutation polynomial on $F_{n\times n}$ iff*

(i) *$f(x)$ is a permutation polynomial on $GF(q),GF(q^2),\ldots,GF(q^n)$, and*

(ii) $f'(x)$ *does not vanish on* $GF(q), GF(q^2),\ldots,GF(q^{[n/2]})$, *where* $[n/2]$ *is the greatest integer in* $n/2$.

Proof. The necessity is clear from the two previous lemmas; thus, assume (i) and (ii) hold and suppose $f(A)=f(B)$ for $A,B\in F_{n\times n}$. Let $E=GF(q^m)$ be the splitting field of $L_n(x)=\prod_{k=1}^{n}(x^{q^k}-x)$, so that $m=$ L.C.M. $\{1,2,\ldots,n\}$ and both A and B have their roots in E; indeed, both A and B have their roots in $\cup_{i=1}^{n}GF(q^i)$, since any irreducible factor $p(x)\in F[x]$ of either of the characteristic polynomials $|xI-A|$ or $|xI-B|$ has degree $k\leqslant n$, implying the roots of $p(x)$ are in $GF(q^k)\subseteq\cup_{i=1}^{n}GF(q^i)$. Now there exist matrices $P,\ Q\in GL(n,E)$ such that

$$P^{-1}AP=\operatorname{diag}(A_1,A_2,\ldots,A_s)=\bar{A} \tag{6.1}$$

and

$$Q^{-1}P^{-1}BPQ=\operatorname{diag}(B_1,B_2,\ldots,B_r)=\bar{B}, \tag{6.2}$$

where $\bar{A}$ and $\bar{B}$ are the Jordan canonical forms of A and B, respectively. Here A_i has the form

$$\operatorname{diag}(J_1(\lambda),J_2(\lambda),\ldots,J_t(\lambda)), \tag{6.3}$$

where each $J_k(\lambda)$ $(k=1,2,\ldots,t)$ is of the form

$$J(\lambda)=\lambda I_v+N_v,$$

N_v being $v\times v$ with 1's on the superdiagonal and 0's elsewhere. Also A_i and A_j correspond to different roots if $i\neq j$. A like statement holds for the B_i's.

Since $f(A)=f(B)$, we have $Q^{-1}f(\bar{A})Q=f(\bar{B})$ or

$$Q^{-1}\operatorname{diag}(f(A_1),\ldots,f(A_s))Q=\operatorname{diag}(f(B_1),\ldots,f(B_r)). \tag{6.4}$$

Now $f(J(\lambda))=f(\lambda)I+f'(\lambda)N_v+c_2N_v^2+\cdots+c_{v-1}N_v^{v-1}$ for some $c_2,\ldots,c_{v-1}\in E$. Here, if $J(\lambda)$ is not 1×1, then there is an elementary divisor of A over $GF(q)$ of the form $p(x)^k$, where $p(x)$ is the minimum polynomial of λ over $GF(q)$ and $k\geqslant 2$. This means $\deg p(x)\leqslant[n/2]$, so that λ is in one of $GF(q),\ldots,GF(q^{[n/2]})$. Therefore $f'(\lambda)\neq 0$. From Sec. 5, Lemma 3, $f(J(\lambda))$ has the Jordan form

$$f(\lambda)I+N_v$$

(which is true even if $v=1$). This means that the Jordan form of either $f(A_i)$ or $f(B_i)$ when A_i or B_i is given by (6.3) is

$$\operatorname{diag}(J_1(f(\lambda)),\ldots,J_t(f(\lambda))).$$

Hence from (6.4) it follows that $s=r$, and that there is some ordering of the B_i's, which we may assume is the order given in (6.2), so that $f(A_i)=f(B_i)$; therefore, $A_i=B_i$, since by condition (i), $f(x)$ is a p.p. on $\cup_{i=1}^{n} GF(q^i)$, in which the roots of A and B lie. Thus $\bar{A}=\bar{B}$, so that

$$P^{-1}AP=\bar{A}=\bar{B}=Q^{-1}P^{-1}BPQ.$$

From (6.4), Q has the form $Q=\text{diag}\,(Q_1,\ldots,Q_r)$, where $f(A_i)Q_i=Q_if(A_i)$. But from Sec. 5, Lemma 2, this means that Q_i commutes with A_i; therefore

$$P^{-1}BP=Q\bar{A}Q^{-1}=\bar{A}=P^{-1}AP,$$

implying $A=B$. Since one-one implies onto, the proof is complete. ■

7. SCALAR PERMUTATION POLYNOMIALS OF $F_{n\times n}$: POLYNOMIAL APPROACH

We now present alternate proofs of the results in Sec. 6. These proofs are given because the new ideas involved are of independent interest. First we give different proofs of Lemmas 1 and 2, Sec. 6.

Let $f(x)\in F[x]$ be a p.p. on $F_{n\times n}$, $F=GF(q)$. From (3.4) and (3.5), there exists a polynomial $g(x)\in F[x]$ such that $g(f(x))\equiv f(g(x))\equiv x \pmod{L_n(x)}$; i.e.,

$$g(f(x))=x+A(x)L_n(x) \tag{7.1}$$

for some $A(x)\in F[x]$. Suppose $f(\alpha)=f(\beta)$ for $\alpha,\ \beta\in GF(q^k)$, $1\leqslant k\leqslant n$. Then since $L_n(\alpha)=L_n(\beta)=0$, we have from (7.1)

$$\alpha=g(f(\alpha))=g(f(\beta))=\beta,$$

which verifies Lemma 1, § 6.

If $P(x)\in F[x]$ is an irreducible of degree k, where $0<2k\leqslant n$, it follows from (7.1) and (3.3) that

$$g(f(x))\equiv x \pmod{P^2(x)}.$$

Differentiating, we get

$$g'(f(x))f'(x)\equiv 1 \pmod{P(x)}$$

and therefore

$$(f'(x),P(x))=1,$$

implying that $f'(x)$ has no roots in $GF(q^k)$, $2k \leqslant n$. This verifies Lemma 2, Sec. 6 and thus proves the necessary part of Theorem 8.

The proof of the sufficiency part is a bit more complicated. Here we will use the following lemma.

LEMMA. *Let $P(x) \in F[x]$ be irreducible of degree k and let $g(x)$, $f(x) \in F[x]$ be such that*

(i) $g(f(x)) \equiv x \pmod{P(x)}$

and

(ii) $(f'(x), P(x)) = 1$.

Then for each integer $m \geqslant 1$ there exists $\Psi_m(x) \in F[x]$ such that

$$\Psi_m(f(x)) \equiv x \pmod{P^m(x)}. \tag{7.2}$$

Proof. The proof is by induction on m. If $m = 1$, we set $\Psi_1(x) = g(x)$; hence, suppose $m > 1$. By the induction assumption there is a $\Psi_{m-1}(x) \in F[x]$ such that

$$\Psi_{m-1}(f(x)) = x + A(x)P^{m-1}(x). \tag{7.3}$$

Consider the polynomial

$$\Psi(x) = \Psi_{m-1}(x) + C(x)(x^{q^k} - x)^{m-1}, \qquad C(x) \in F[x].$$

Now

$$\Psi(f(x)) = \Psi_{m-1}(f(x)) + C(f(x))\left(f^{q^k}(x) - f(x)\right)^{m-1}$$

$$= x + A(x)P^{m-1}(x) + C(f(x))\left(f^{q^k}(x) - f(x)\right)^{m-1}.$$

Note that $P^{m-1}(x) | (f^{q^k}(x) - f(x))^{m-1}$, since if $\theta \in GF(q^k)$ satisfies $P(\theta) = 0$, then $f^{q^k}(\theta) - f(\theta) = 0$ implies $P(x) | (f^{q^k}(x) - f(x))$. Moreover, by (ii)

$$\frac{f^{q^k}(x) - f(x)}{P(x)}\Big|_{x=\theta} = \frac{-f'(\theta)}{P'(\theta)} \neq 0,$$

so that

$$\frac{f^{q^k}(x) - f(x)}{P(x)} = B(x), \qquad (B(x), P(x)) = 1.$$

Clearly $\Psi(x)$ will satisfy (7.2) provided

$$A(x)+C(f(x))B^{m-1}(x)\equiv 0 \pmod{P(x)} \tag{7.4}$$

or

$$C(f(x))=-[B^{m-1}(x)]^{-1}A(x), \pmod{P(x)}.$$

By (i), $C(x)$ exists, and the proof is complete. ∎

It is clear from (3.4) that the next theorem is just a restatement of the sufficiency part of Theorem 8.

THEOREM 9. *Let n be a fixed positive integer and let $f(x)\in F[x]$ be a polynomial such that*

(i) *$f(x)$ is a permutation polynomial on $GF(q)$, $GF(q^2),\dots,GF(q^n)$ and*
(ii) *$f'(x)$ does not vanish on $GF(q)$, $GF(q^2),\dots,GF(q^{[n/2]})$.*

Then there exists a polynomial $\psi(x)$ such that

$$\Psi(f(x))\equiv x \pmod{L_n(x)},$$

where $L_n(x)$ is given by (3.2).

Proof. Consider first an arbitrary irreducible monic $P(x)\in F[x]$ of degree k, where $1\leqslant k\leqslant n$. Since by (3.3)

$$L_n(x)=\prod_{\deg Q=k\leqslant n} Q(x)^{[n/k]},$$

where the product is over all irreducible monics $Q(x)\in F[x]$ of degree $\leqslant n$, $P(x)$ is a factor of $L_n(x)$. In particular, if $k>n/2$, then $P(x)$ is a simple factor, as $[n/k]=1$.

Now consider a polynomial $f(x)\in F[x]$ satisfying hypotheses (i) and (ii). Since $f(x)$ is a p.p. on $GF(q^k)$, $1\leqslant k\leqslant n$, it belongs to the finite group of all permutations of $GF(q^k)$. Thus, there exist a polynomial $g(x)\in F[x]$ which defines the inverse of $f(x)$ acting on $GF(q^k)$; indeed, $g(x)$ can be taken as $f(f(\dots f(x)))$ modulo $(x^{q^k}-x)$ for some finite number of compositions. Hence

$$f(g(\lambda))=g(f(\lambda))=\lambda, \qquad \lambda\in GF(q^k),$$

which implies that

$$f(g(x))\equiv g(f(x))\equiv x \pmod{P(x)} \tag{7.5}$$

for an arbitrary irreducible monic $P(x)\in F[x]$ of degree k.

We can now deduce that for an arbitrary monic irreducible $P(x)$ of degree $k \leqslant n$ there exists a polynomial $\psi_P(x) \in F[x]$, which may depend on $P(x)$, such that

$$\psi_P(f(x)) \equiv x \left(\mathrm{mod}\, P(x)^{[n/k]}\right). \tag{7.6}$$

To see this, note that if $k > n/2$, then $[n/k] = 1$, so that we may take as $\psi_P(x)$ the $g(x)$ of (7.5). If, however, $k \leqslant n/2$, then from (7.5) and the fact that $(f'(x), P(x)) = 1$ (otherwise $f'(x)$ would vanish in $GF(q^k)$), we may apply the above Lemma to obtain (7.6). Now (7.6) means that the polynomial $f(x)$, viewed as a function on the quotient ring $F[t]/(P(t)^{[n/k]})$, is a permutation with inverse $\psi_P(x)$; hence

$$f(\psi_P(x)) \equiv X \left(\mathrm{mod}\, P(x)^{[n/k]}\right).$$

By the Chinese remainder theorem there is a unique $\mathrm{mod}\, L_n(x)$ solution to the system of congruences

$$\psi(x) \equiv \psi_P(x) \left(\mathrm{mod}\, P(x)^{[n/k]}\right).$$

Now

$$f(\psi(x)) \equiv f(\psi_P(x)) \equiv x \left(\mathrm{mod}\, P(x)^{[n/k]}\right);$$

thus

$$f(\psi(x)) \equiv x \,(\mathrm{mod}\, L_n(x)).$$

It follows that $\psi(f(x)) \equiv x \,(\mathrm{mod}\, L_n(x))$, and the proof is complete. ■

REFERENCES

1 J. V. Brawley and L. Carlitz, A characterization of the $n \times n$ matrices over a finite field, *Amer. Math. Monthly* **80** (1973), pp. 670–672.

2 L. Carlitz, On polynomials in a Galois field, *Bull. Amer. Math. Soc.* **38** (1932), pp. 736–744.

3 L. E. Dickson, *Linear Groups with an Exposition of Galois Field Theory*, Dover, New York, 1958.

4 O. Ore, On a special class of polynomials, *Amer. Math. Soc. Trans.* **35** (1933), pp. 559–584.

5 O. Ore, Contributions to the theory of finite fields, *Amer. Math. Soc. Trans.* **36** (1934), pp. 243–274.

6 Sam Perlis, Theory of Matrices, Addison-Wesley, Reading, Mass., 1952.

7 L. Rédei, *Algebra*, Vol. 1, Pergamon Press, Oxford, 1967.

8 H. W. Turnbull and A. C. Aitken, *An Introduction to the Theory of Canonical Matrices*, Dover, New York, 1961.

Received 20 August 1973; revised March 1974